Practical Exercise

Kevin Theuermann

kevin.theuermann@egiz.gv.at

EGIZ

E-Government
Innovationszentrum

E-Government | Practical Exercise

Kevin Theuermann
kevin.theuermann@egiz.gv.at

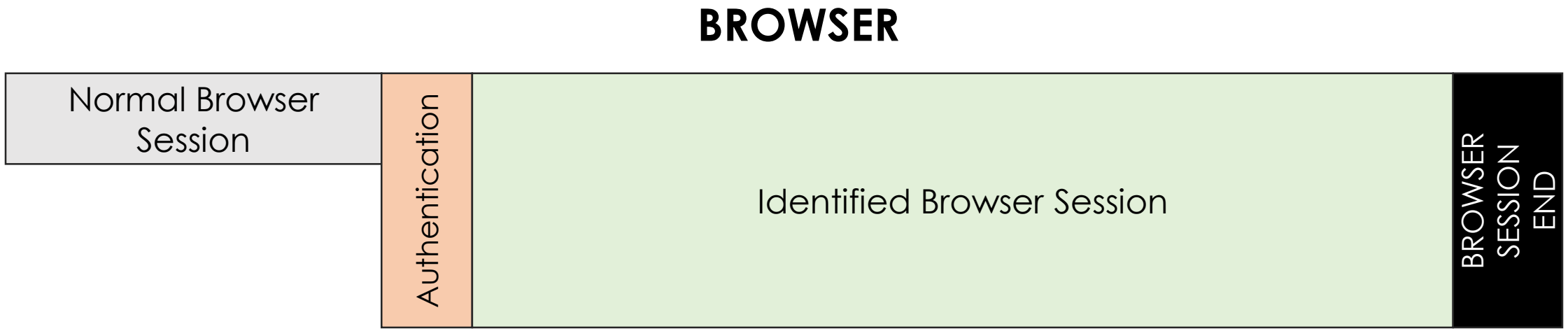
E-Government | Authentication via Username/Password

- 1-Factor-Authentication: Knowledge
- Passwords/PINs can be forgotten/stolen
- Not secure enough for E-government applications
- Can be easily hacked with today's computing possibilities

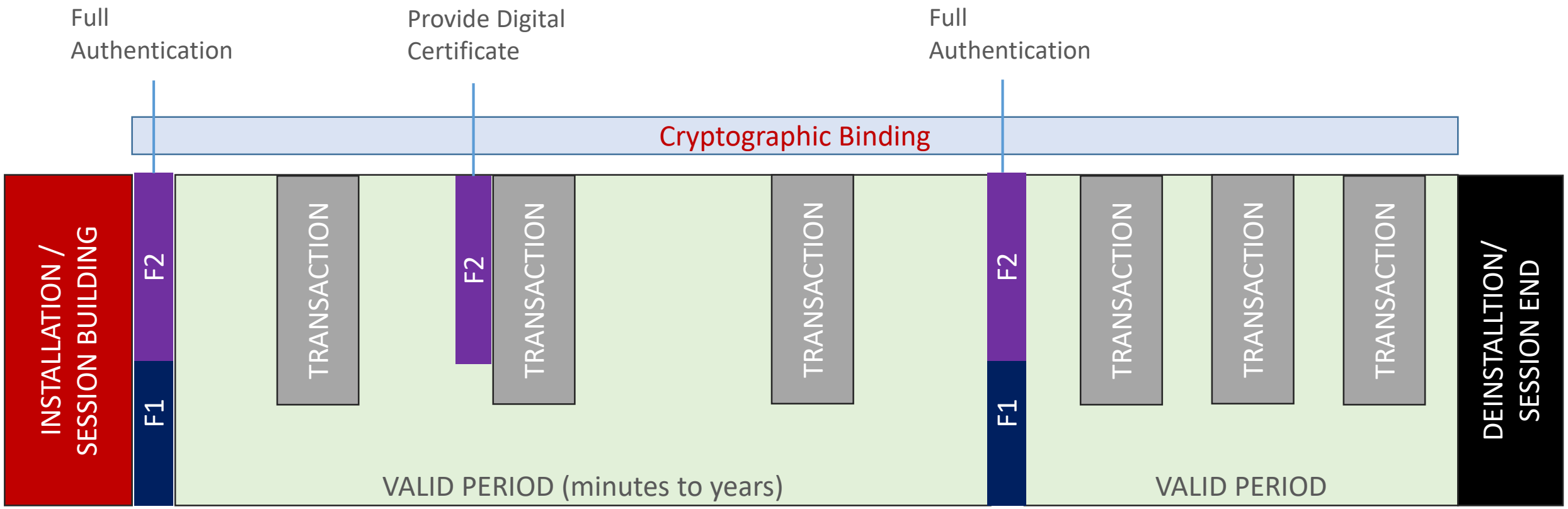
E-Government | Authentication Solution

- Using Multifactor-Authentication: Knowledge + Possession
- Using digital cryptographic certificates and signatures (client TLS)
- Using the possibilities offered by smartphones
- Cryptographic Binding between Person, Mobile Device and Online Application

E-Government | Authentication Solution



E-Government | Authentication Solution



Client TLS Authentication | Minimal Criteria

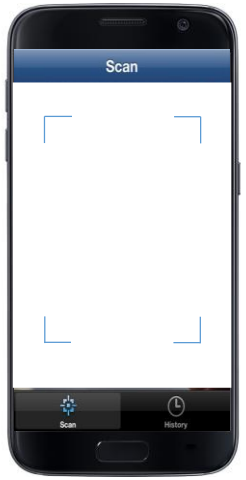
1

Login via Citizen Card/ Mobile Phone Signature

2

QR-Code will be displayed after successful login

3



QR-Code must be scanned via smartphone app

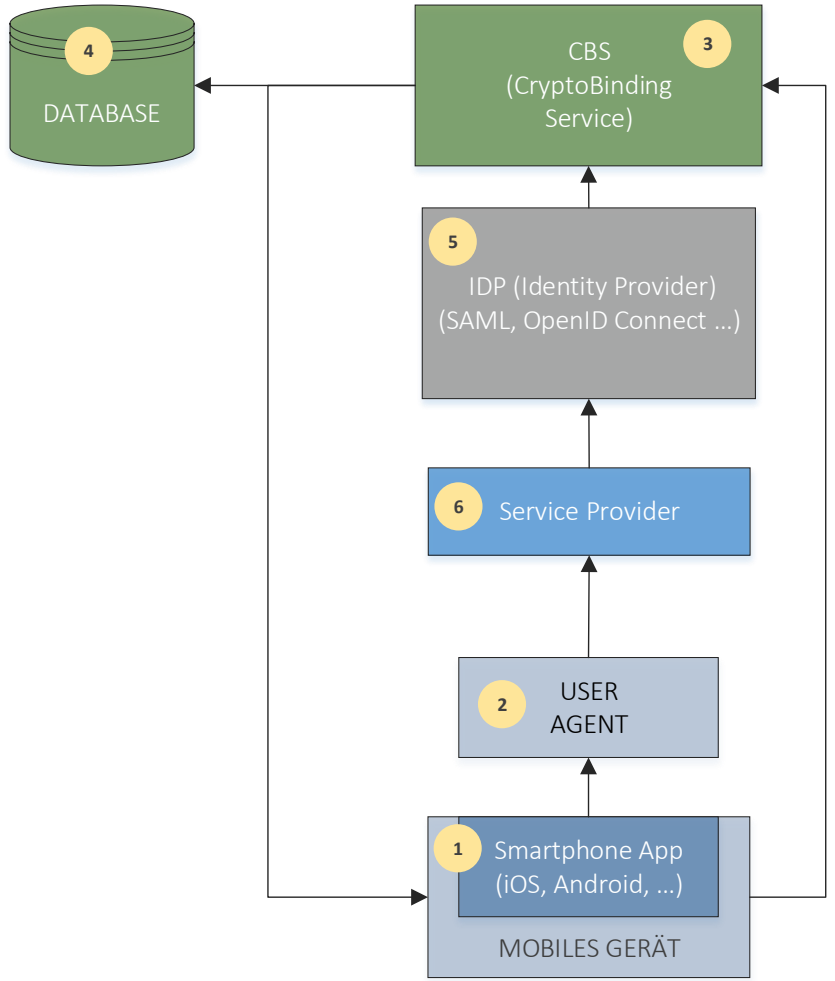
4

Client TLS Auth. with Service Provider

https://apps.egiz.gv.at/tokenservice/token

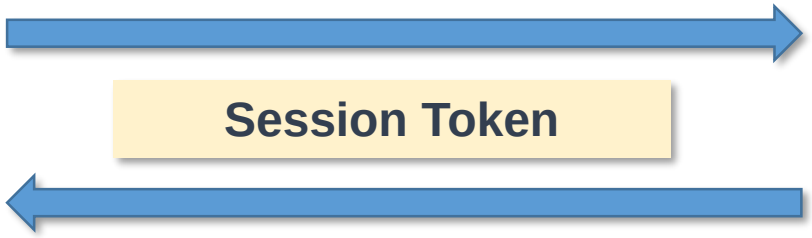
E-Government | Client TLS Authentication Components

1. **Smartphone App:** The app that has to be developed. Through this app the client TLS authentication should be enabled.
2. **User Agent:** The browser respectively the webview component, by which the final service should be accessed/consumed.
3. **CryptoBinding – Service:** The service responsible for implementing cryptographical bindings and issuing of certificates.
4. **Database:** The component where the cryptographic certificates will be stored.
5. **Identity Provider:** The party which provides an authentication system. The CryptoBinding-Service is provided by the IDP.
6. **Service Provider:** The party which provides a digital service and requires an authentication of users.



Client TLS Authentication | Minimal Criteria

QR Code: Session Token + URL to IDP



Session Token

Cryptographic Information

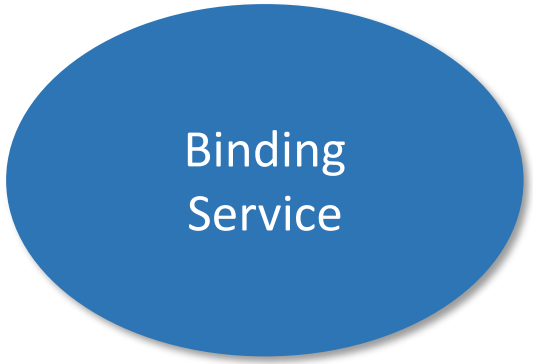
Binding Service

Client TLS Authentication | Minimal Criteria

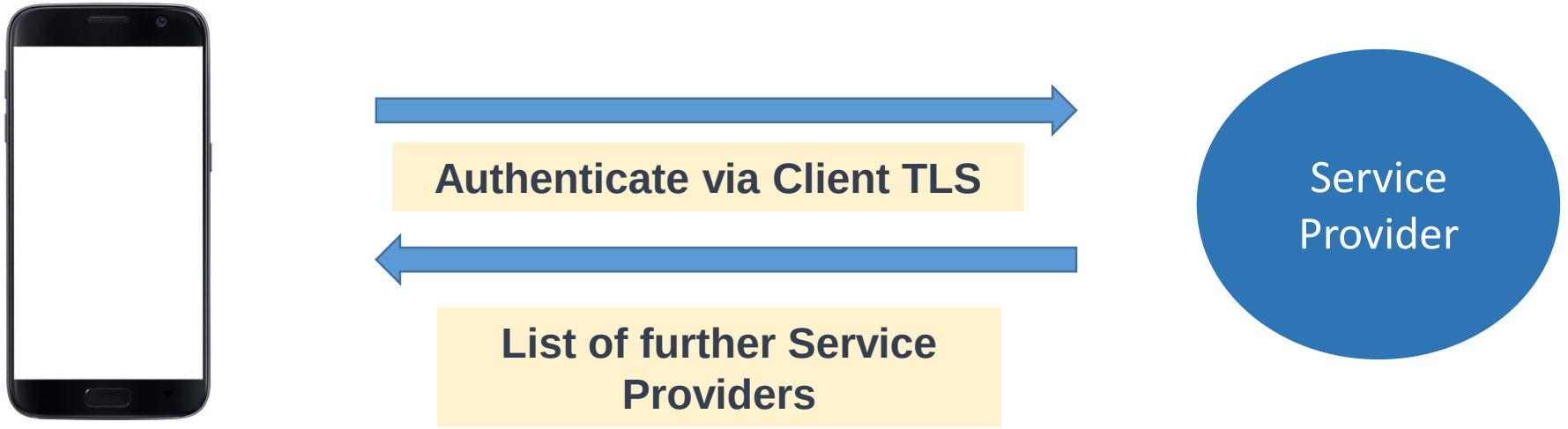
Generate Public/Private Keypair + Certificate Signing Request (CSR)

Certificate Signing Request

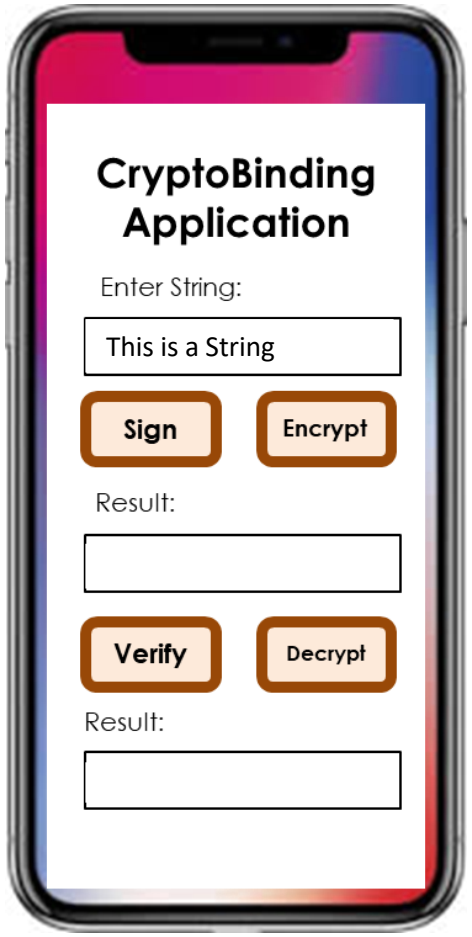
Cryptographic Certificate



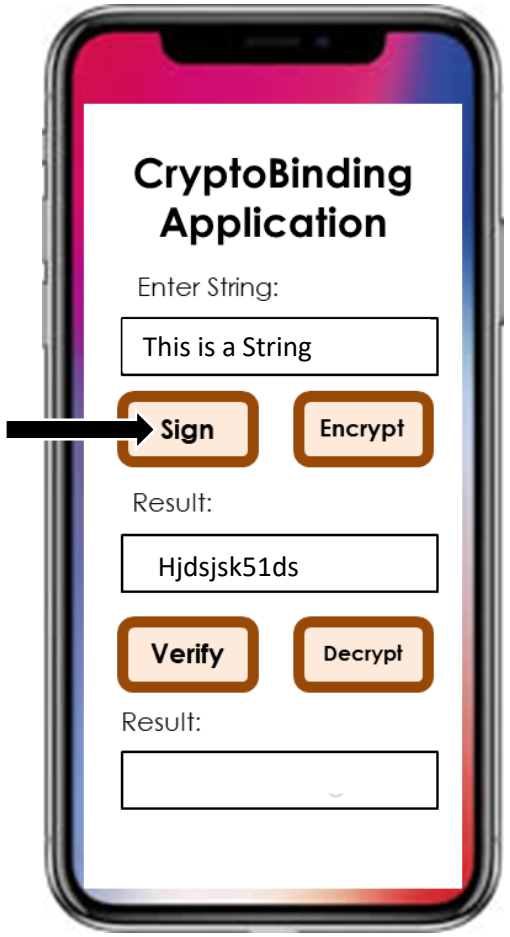
Client TLS Authentication | Minimal Criteria



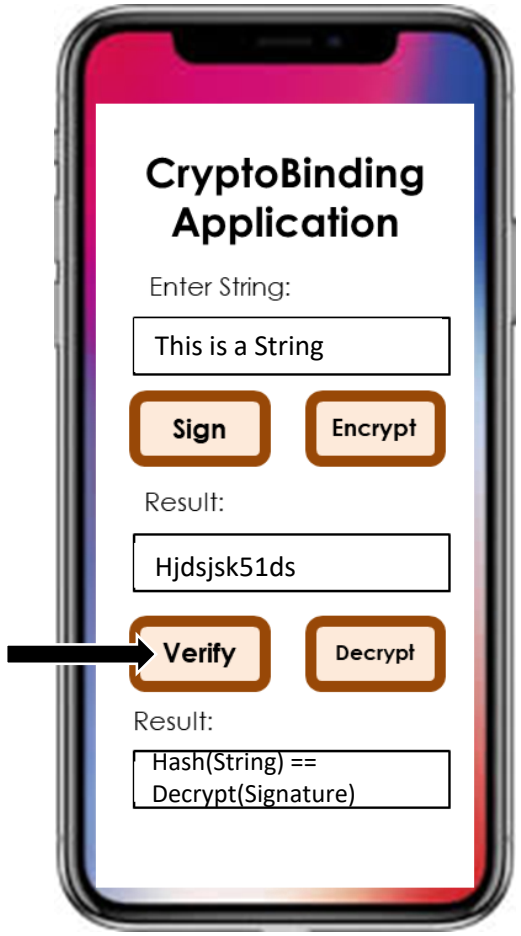
Key Management | Signing



STEP 1

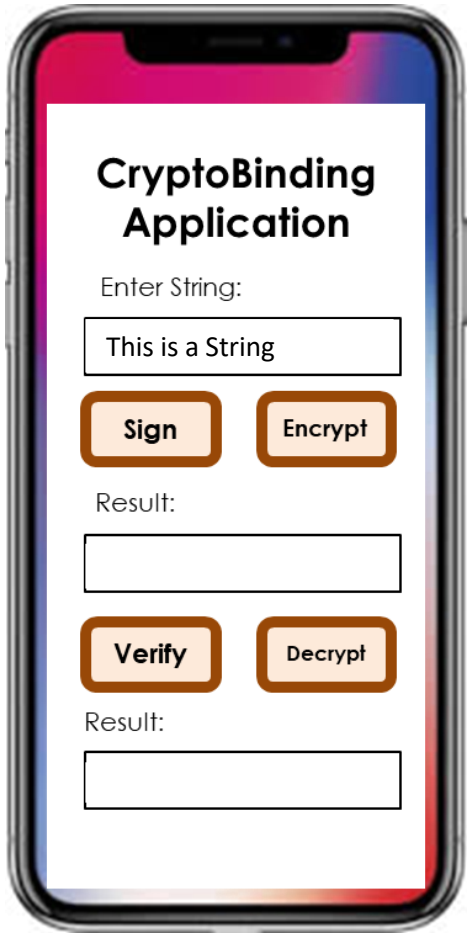


STEP 2

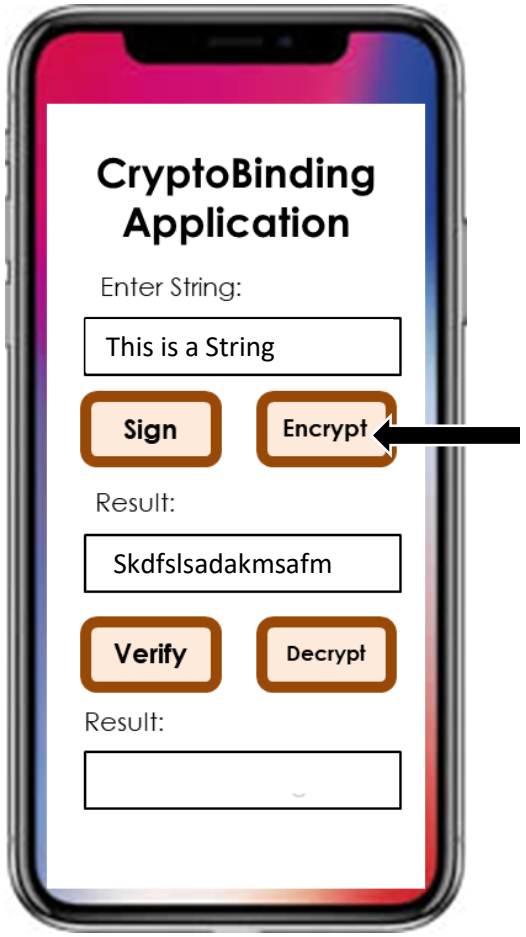


STEP 3

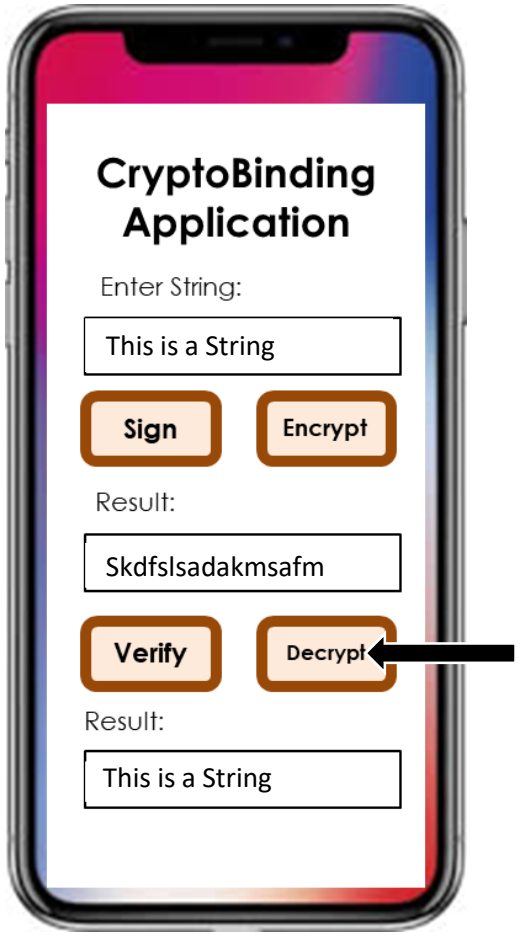
Key Management | Encryption/Decryption



STEP 1



STEP 2



STEP 3

E-Government | Grading Criteria and Minimal Requirements

- Minimal Requirement (Sufficient): Perform cryptographic binding according to the documentation provided at: https://teaching.iaik.tugraz.at/egov/practicals
- In order to get a better grade the development process can be extended as described in the practical exercise documentation
- If another's code has been used, the delivery of the practical exercise is invalid

E-Government | General Notes

- Programming exercise
- Individual work
- Operating System: iOS or Android
- Developing Environment: XCode, Android Studio, whatever you prefer

E-Government | Further General Information

- Send the application to kevin.theuermann@egiz.gv.at until the 09.01.2020
- Compulsory meetings for discussing the assignments (”Abgabegespräche”) will be announced during the semester
- For important questions, contact me directly: kevin.theuermann@egiz.gv.at